

Formal groups and congruences

Masha Vlasenko

September 2, 2016

We give a criterion of integrality of an one-dimensional formal group law in terms of congruences satisfied by the coefficients of the canonical invariant differential. For an integral formal group law a p -adic analytic formula for the local characteristic polynomial at p is given. We demonstrate applications of our results to formal group laws attached to L-functions, Artin–Mazur formal groups of algebraic varieties and hypergeometric formal group laws.

1 Introduction

Let R be a commutative ring with the identity. A formal group law of dimension 1 over R is a power series in two variables $F(x, y) \in R[[x, y]]$ satisfying the conditions

$$\begin{aligned} F(x, 0) &= F(0, x) = x, \\ F(F(x, y), z) &= F(x, F(y, z)). \end{aligned}$$

A formal group law is said to be commutative when $F(x, y) = F(y, x)$. For two formal group laws F_1 and F_2 over R and a ring $R' \supseteq R$, a homomorphism $h \in \text{Hom}_{R'}(F_1, F_2)$ is a power series $h \in xR'[[x]]$ such that $h(F_1(x, y)) = F_2(h(x), h(y))$. An invertible homomorphism is called an isomorphism. An isomorphism h is called strict if $h(x) \equiv x$ modulo degree ≥ 2 .

From now on we assume that R is a characteristic zero ring (i.e. $R \rightarrow R \otimes \mathbb{Q}$ is injective). In this case every formal group law $F \in R[[x, y]]$ is commutative and strictly isomorphic over $R \otimes \mathbb{Q}$ to the trivial formal group law $\mathbb{G}_a(x, y) = x + y$. The unique strict isomorphism $f \in \text{Hom}_{R \otimes \mathbb{Q}}(F, \mathbb{G}_a)$ is called the logarithm of F . The logarithm satisfies

$$F(x, y) = f^{-1}(f(x) + f(y)) \tag{1}$$

and can be written in the form

$$f(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} x^n \tag{2}$$

with $b_n \in R$, $b_0 = 1$. The shift in indices (b_{n-1} instead of b_n) looks more natural in the view of the fact that $f'(x)dx = \sum_{n=0}^{\infty} b_n x^n dx$ is the canonical invariant differential on F ([2], [1, §5.8]). We shall characterize those R -valued sequences $\{b_n; n \geq 0\}$ which arise as sequences of coefficients of canonical differentials on one-parameter formal group laws over R . This question is trivial when $R = R \otimes \mathbb{Q}$, in which case any sequence $\{b_n; n \geq 0\}$ yields a formal group law over R by formulas (1) and (2).

Fix a prime number p and assume that R is equipped with a p th power Frobenius endomorphism $\sigma : R \rightarrow R$ (i.e. $\sigma(r) \equiv r^p \pmod{pR}$). We extend σ to polynomials $R[x]$ and power series $R[[x]]$ by assigning $\sigma(x) = x^p$. Our first result (Theorem 1 below) gives a necessary and sufficient condition for the sequence $\{b_n; n \geq 0\}$ under which p doesn't show up in the denominators in (1). In order to state this criterion we need to define a transformation of the sequence

$\{b_n; n \geq 0\}$. For a non-negative integer n we will denote by $\ell(n) = \min\{s \geq 1 : n < p^s\}$ the length of the p -adic expansion of n . For two non-negative integers n, m we denote by $n * m$ the integer whose p -adic expansion is the concatenation of the p -adic expansions of n and m respectively, that is $n * m = n + m p^{\ell(n)}$. Notice that $n * 0 = n$ and $\ell(n * m) = \ell(n) + \ell(m)$ if and only if $m > 0$.

Definition. Let $\{b_n; n \geq 0\}$ be a sequence of elements of R . The p -sequence associated to $\{b_n; n \geq 0\}$ is the sequence of elements of R given by

$$c_n = \sum_{\substack{n = n_1 * \dots * n_k \\ n_1 \geq 0, n_2, \dots, n_k > 0}} (-1)^{k-1} b_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}) \cdot \sigma^{\ell(n_1)+\ell(n_2)}(b_{n_3}) \cdot \dots \cdot \sigma^{\ell(n_1)+\dots+\ell(n_{k-1})}(b_{n_k})$$

for $n \geq 0$, where the sum runs over all possible decompositions of the p -adic expansion of n into a tuple of p -adic expansions of non-negative integers.

The original sequence $\{b_n; n \geq 0\}$ can be reconstructed from its p -sequence, hence any R -valued sequence can occur as a p -sequence associated to an R -valued sequence (see Section 2 for details). To author's knowledge, p -sequences were first introduced by Anton Mellit in [5] motivated by the result which we will reproduce later (Proposition 4 in Section 4.2) in a slightly more general form.

Theorem 1. Let R be a characteristic zero ring (i.e. $R \rightarrow R \otimes \mathbb{Q}$ is injective) endowed with a p th power Frobenius endomorphism $\sigma : R \rightarrow R$ (i.e. $\sigma(r) \equiv r^p \pmod{pR}$ for every $r \in R$). Let $\{b_n; n \geq 0\}$ be a sequence of elements of R with $b_0 = 1$. Put $f(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} x^n$. The formal group law $F(x, y) = f^{-1}(f(x) + f(y))$ has coefficients in $R \otimes \mathbb{Z}_{(p)}$ if and only if the p -sequence $\{c_n; n \geq 0\}$ associated to $\{b_n; n \geq 0\}$ satisfies

$$c_{mp^k-1} \in p^k R \quad \text{for all } m > 1, k \geq 0. \quad (3)$$

The reader may notice that the statement of the theorem is trivial when p is invertible in R , in which case $R \otimes \mathbb{Z}_{(p)} = R \otimes \mathbb{Q}$. Since $\cap_p(R \otimes \mathbb{Z}_{(p)}) = R$, the following global criterion follows immediately.

Corollary. Let R be a characteristic zero ring endowed with a p th power Frobenius morphism for every rational prime p . Let $\{b_n; n \geq 0\}$ be a sequence of elements of R with $b_0 = 1$. In the notation of Theorem 1, we have $F(x, y) \in R[[x, y]]$ if and only if for every p the respective p -sequence $\{c_n; n \geq 0\}$ (it is a different one for each p) associated to $\{b_n; n \geq 0\}$ satisfies (3).

We prove Theorem 1 in Section 2. The proof is based on Hazewinkel's functional equation lemma ([1, §2.2]). By [1, Proposition 20.1.3] every formal group law over a $\mathbb{Z}_{(p)}$ -algebra is of functional equation type. In our case it means that $F(x, y)$ has coefficients in $R \otimes \mathbb{Z}_{(p)}$ if and only if there exists a sequence of elements $v_1, v_2, \dots \in R \otimes \mathbb{Z}_{(p)}$ such that the series

$$g(x) = f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s \cdot (\sigma^s f)(x) \quad (4)$$

has coefficients in $R \otimes \mathbb{Z}_{(p)}$. Such a sequence $\{v_s; s \geq 1\}$ is non-unique. Our proof shows that one of possible choices is given by $v_s = \frac{c_{p^s-1}}{p^{s-1}} \in R$.

From now on let us assume that R is the ring of integers of a complete absolutely unramified discrete valuation field of characteristic zero and residue characteristic $p > 0$, equipped with

a lift $\sigma : R \rightarrow R$ of the p th power Frobenius on the residue field R/pR . In this case one can construct the *shortest possible* functional equation (4) for the logarithm $f(x)$ of a formal group law $F(x, y) \in R[[x, y]]$. Namely, suppose we have any functional equation (4) and let

$$h = \inf\{s \geq 1 : v_s \in R^\times\}. \quad (5)$$

If $h = \infty$ then $f(x) \in R[[x]]$ and hence F is strictly isomorphic to \mathbb{G}_a over R . If $h < \infty$ then there exist unique $\alpha_1, \dots, \alpha_{h-1} \in pR$ and $\alpha_h \in R^\times$ such that

$$f(x) - \frac{1}{p} \sum_{s=1}^h \alpha_s \cdot (\sigma^s f)(x) \in R[[x]].$$

The Eisenstein polynomial

$$\Psi_F(T) = p - \sum_{i=1}^h \alpha_i T^i \in R[T]$$

is called the *characteristic polynomial* of $F(x, y)$ and h is called the *height*. Two formal group laws over R are strictly isomorphic if and only if their characteristic polynomials are equal ([2, Proposition 3.5], [1, Theorem 20.3.12]). By convention, we put $\Psi_F(T) = p$ if $h = \infty$.

In the case when the residue field is finite ($\#R/pR = q = p^f$) the above defined height coincides with the height of the multiplication by p endomorphism $[p]_{\overline{F}}$ of the reduction $\overline{F}(x, y) \in \mathbb{F}_q[[x, y]]$. However $\Psi_F(T)$ shall not be confused with the characteristic polynomial of the Frobenius endomorphism $\xi_{\overline{F}}(x) = x^q$. When $R = \mathbb{Z}_p$ then $\alpha_h^{-1} \Psi_F(T)$ coincides with the characteristic polynomial of $\xi_{\overline{F}}$, but in general the relation between these two invariants is more subtle (see [1, §30.4, Remark 18.5.13]).

The following theorem describes congruences satisfied by the coefficients of the logarithm of an integral formal group law and provides a p -adic analytic formula for the characteristic polynomial.

Theorem 2. *Let R be the ring of integers of a complete absolutely unramified discrete valuation field of characteristic zero and residue characteristic $p > 0$, equipped with a lift $\sigma : R \rightarrow R$ of the p th power Frobenius on the residue field R/pR . Let $F(x, y) \in R[[x, y]]$ be a formal group law of height h . When $h < \infty$ we denote by $\Psi_F(T) = p - \sum_{i=1}^h \alpha_i T^i \in R[T]$ the characteristic polynomial of F . We write the logarithm of F in the form*

$$\log_F(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} x^n,$$

where $\{b_n; n \geq 0\}$ is a sequence of elements of R with $b_0 = 1$.

(i) If $h = \infty$ then $\text{ord}_p(b_{p^n-1}) \geq n$ for all n .

If $h < \infty$ then $\text{ord}_p(b_{p^n-1}) \geq n - \lfloor \frac{n}{h} \rfloor$ with equality when $h|n$.

(ii) When $h < \infty$, consider elements $\beta_n = b_{p^n-1}/p^{n-\lfloor \frac{n}{h} \rfloor} \in R$. We have

$$\beta_{kh} \equiv \prod_{i=0}^{k-1} \sigma^{ih}(\beta_h) \pmod{p}.$$

(iii) When $h < \infty$, consider for every $k \geq 1$ an $h \times h$ matrix with coefficients in R given by

$$D_k = \left(p^{\varepsilon_{ij}} \sigma^{j+1}(\beta_{kh-1+i-j}) \right)_{0 \leq i, j \leq h-1} \quad \text{with} \quad \varepsilon_{ij} = \begin{cases} 0, & j < i \text{ or } j = h-1, \\ 1, & i \leq j < h-1. \end{cases}$$

We have that $\det D_k \equiv (-1)^{h-1} \prod_{s=1}^{kh-1} \sigma^s(\beta_h) \neq 0 \pmod{p}$ and

$$\begin{pmatrix} \alpha_1/p \\ \alpha_2/p \\ \vdots \\ \alpha_{h-1}/p \\ \alpha_h \end{pmatrix} \equiv D_k^{-1} \begin{pmatrix} \beta_{kh} \\ \beta_{kh+1} \\ \vdots \\ \beta_{kh+h-2} \\ \beta_{kh+h-1} \end{pmatrix} \pmod{p^k}. \quad (6)$$

For example, it follows from (i) that the height is equal to 1 if and only if $p \nmid b_{p-1}$. In this case we have that $p \nmid b_{p^k-1}$ for all $k \geq 1$ and there exists a unique unit $\alpha_1 \in R^\times$ such that for every $k \geq 1$

$$b_{p^k-1}/\sigma(b_{p^{k-1}-1}) \equiv \alpha_1 \pmod{p^k}. \quad (7)$$

The characteristic polynomial is given by $\Psi_F(T) = p - \alpha_1 T$.

In the case of height 2, we have $\text{ord}_p(b_{p^{2k}-1}) = k$ and $\text{ord}_p(b_{p^{2k-1}-1}) \geq k$ for all k by (i), and (iii) gives us the following formulas for the coefficients of the characteristic polynomial $\Psi_F(T) = p - \alpha_1 T - \alpha_2 T^2$:

$$\begin{pmatrix} \frac{\alpha_1}{p} \\ \alpha_2 \end{pmatrix} \equiv \begin{pmatrix} p \frac{\sigma(b_{p^{2k-1}-1})}{p^k} & \frac{\sigma^2(b_{p^{2k-2}-1})}{p^{k-1}} \\ \frac{\sigma(b_{p^{2k-1}-1})}{p^k} & \frac{\sigma^2(b_{p^{2k-1}-1})}{p^k} \end{pmatrix}^{-1} \begin{pmatrix} \frac{b_{p^{2k}-1}}{p^k} \\ \frac{b_{p^{2k+1}-1}}{p^{k+1}} \end{pmatrix} \pmod{p^k}$$

or, equivalently,

$$\begin{aligned} \alpha_1 &\equiv \frac{\sigma^2(b_{p^{2k-1}-1}) b_{p^{2k}-1} - \sigma^2(b_{p^{2k-2}-1}) b_{p^{2k+1}-1}}{\sigma(b_{p^{2k-1}-1}) \sigma^2(b_{p^{2k-1}-1}) - \sigma(b_{p^{2k}-1}) \sigma^2(b_{p^{2k-2}-1})} \pmod{p^k}, \\ \alpha_2 &\equiv \frac{1}{p} \frac{\sigma(b_{p^{2k-1}-1}) b_{p^{2k+1}-1} - \sigma(b_{p^{2k}-1}) b_{p^{2k}-1}}{\sigma(b_{p^{2k-1}-1}) \sigma^2(b_{p^{2k-1}-1}) - \sigma(b_{p^{2k}-1}) \sigma^2(b_{p^{2k-2}-1})} \pmod{p^k}. \end{aligned} \quad (8)$$

We prove Theorem 2 in Section 3. Section 4 is devoted to applications of our theorems. We start with formal group laws attached to L -functions. In this case the p -sequence recovers coefficients of the respective local L -factor at p and there are finitely many non-zero congruences (3) to be checked. In Section 4.2 we show that Theorem 1 implies integrality of certain Artin–Mazur formal groups arising from cohomology of algebraic varieties. In this situation Theorem 2 is useful for computation of eigenvalues of the Frobenius operator on the respective crystalline (or ℓ -adic) cohomology group. In Section 4.3 we give a criterion of integrality and compute local characteristic polynomials of hypergeometric formal group laws generalizing the results in [4]. Here again the criterion in Theorem 1 can be reduced to finitely many congruences.

Acknowledgement. The criterion of integrality (Theorem 1) was initially conjectured by Eric Delaygue during our correspondence. I would like to thank Eric for numerous fruitful discussions of the subject. I am also grateful to Piotr Achinger and Susanne Müller, whose remarks helped to improve the exposition.

2 A criterion of integrality of a formal group law

This section is devoted to the proof of Theorem 1. We recall that R is a ring of characteristic zero endowed with a morphism $\sigma \in \text{End}(R)$ satisfying $\sigma(r) \equiv r^p \pmod{pR}$ for any $r \in R$. We extend σ to a p th power Frobenius morphism of $R \otimes \mathbb{Q}$ by \mathbb{Q} -linearity and further to the ring of power series in x with coefficients in $R \otimes \mathbb{Q}$ by assigning $\sigma(x) = x^p$. For a sequence $\{b_n; n \geq 0\}$ of elements of R the respective p -sequence was defined as

$$c_n = \sum_{\substack{n = n_1 * \dots * n_k \\ n_1 \geq 0, n_2, \dots, n_k > 0}} (-1)^{k-1} b_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}) \cdot \sigma^{\ell(n_1)+\ell(n_2)}(b_{n_3}) \cdot \dots \cdot \sigma^{\ell(n_1)+\dots+\ell(n_{k-1})}(b_{n_k}). \quad (9)$$

When $k = 1$ we have $n = n_1 \geq 0$ and the condition $n_2, \dots, n_k > 0$ is empty. This is a finite sum because $k \leq \ell(n)$. We will start with discussing some properties of p -sequences. For small indices we have

$$\begin{aligned} c_0 &= b_0, \quad c_1 = b_1, \quad \dots, \quad c_{p-1} = b_{p-1}, \\ c_p &= b_p - b_0 \sigma(b_1), \quad c_{1+p} = b_{1+p} - b_1 \sigma(b_1), \quad \dots \\ c_{p^2} &= b_{p^2} - b_0 \sigma(b_p), \quad c_{1+p^2} = b_{1+p^2} - b_1 \sigma(b_p), \quad \dots \\ c_{p+p^2} &= b_{p+p^2} - b_0 \sigma(b_{1+p}) - b_p \sigma^2(b_1) + b_0 \sigma(b_1) \sigma^2(b_1), \quad \dots \end{aligned}$$

One can easily notice that the original sequence $\{b_n; n \geq 0\}$ can be reconstructed from its p -sequence $\{c_n; n \geq 0\}$ since the right-hand side of (9) is the sum of b_n and an expression containing only b_k with $k < n$.

Lemma. *We have $b_0 = c_0$ and*

$$b_n = \sum_{\substack{n = n_1 * (\dots * (n_{k-1} * n_k) \dots) \\ n_k > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(c_{n_2}) \cdot \sigma^{\ell(n_1)+\ell(n_2)}(c_{n_3}) \cdot \dots \cdot \sigma^{\ell(n_1)+\dots+\ell(n_{k-1})}(c_{n_k})$$

for every $n > 0$.

Proof. Observe that

$$\begin{aligned} c_n &= \sum_{\substack{n = n_1 * \dots * n_k \\ n_1 \geq 0, n_2, \dots, n_k > 0}} (-1)^{k-1} b_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}) \cdot \sigma^{\ell(n_1)+\ell(n_2)}(b_{n_3}) \cdot \dots \cdot \sigma^{\ell(n_1)+\dots+\ell(n_{k-1})}(b_{n_k}) \\ &= b_n - \sum_{\substack{n = n_1 * n_2 \\ n_2 > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}), \end{aligned}$$

and therefore

$$\begin{aligned} b_n &= c_n + \sum_{\substack{n = n_1 * n_2 \\ n_2 > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}) \\ &= c_n + \sum_{\substack{n = n_1 * n_2 \\ n_2 > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(c_{n_2}) + \sum_{\substack{n = n_1 * (n_2 * n_3) \\ n_3 > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(c_{n_2}) \cdot \sigma^{\ell(n_1)+\ell(n_2)}(b_{n_3}) \\ &= \dots, \end{aligned}$$

which yields the statement of the lemma by iteration. \square

In what follows we will often use the following relation between the p -sequence and the original sequence, which we extract from the proof of the above lemma:

$$b_n = c_n + \sum_{\substack{n = n_1 * n_2 \\ n_2 > 0}} c_{n_1} \cdot \sigma^{\ell(n_1)}(b_{n_2}). \quad (10)$$

Proof of Theorem 1. \Leftarrow Assume that (3) holds, so we have

$$c_{mp^k-1} \in p^k R \text{ for all } m > 1, k \geq 0. \quad (11)$$

For $s \geq 1$ consider elements $v_s = \frac{1}{p^{s-1}} c_{p^s-1}$ which lie in R due to (11). Consider the power series

$$\sum_{n=1}^{\infty} d_n x^n = f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s \cdot (\sigma^s f)(x). \quad (12)$$

For each n , write $n = mp^k$ with $k \geq 0$ and $(m, p) = 1$. If $k = 0$ then $d_n = \frac{1}{n} b_{n-1} \in R \otimes \mathbb{Z}_{(p)}$. If $k > 0$ we have

$$\begin{aligned} d_n &= \frac{1}{mp^k} b_{mp^k-1} - \frac{1}{p} \sum_{i=1}^k v_i \cdot \frac{1}{mp^{k-i}} \sigma^i(b_{mp^{k-i}-1}) \\ &= \frac{1}{mp^k} \left(b_{mp^k-1} - \sum_{i=1}^k c_{p^i-1} \cdot \sigma^i(b_{mp^{k-i}-1}) \right) \\ &= \frac{1}{mp^k} \sum_{\substack{m = m' * m'' \\ m' > 1}} c_{m'p^k-1} \cdot \sigma^{k+\ell(m')}(b_{m''}), \end{aligned}$$

where the sum is over all possible decompositions $m = m' + m'' p^{\ell(m')}$ with $m' > 1$. If $m = 1$ the sum is simply 0. If $m > 1$ then we have $c_{m'p^k-1} \in p^k R$ for every term in the sum due to (11), and therefore $d_n \in R \otimes \mathbb{Z}_{(p)}$. We proved that (12) is a series with coefficients in $R \otimes \mathbb{Z}_{(p)}$, and therefore $F(x, y)$ has coefficients in the same ring by Hazewinkel's functional equation lemma ([1, §2.2]).

\Rightarrow Suppose $F(X, Y)$ has coefficients in $R \otimes \mathbb{Z}_{(p)}$. By [1, Proposition 20.1.3] every formal group law over a $\mathbb{Z}_{(p)}$ -algebra is of functional equation type. This means that there exist elements $v_1, v_2, \dots \in R \otimes \mathbb{Z}_{(p)}$ such that the series

$$\sum_{n=1}^{\infty} d_n x^n = f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s \cdot (\sigma^s f)(x)$$

has coefficients in $R \otimes \mathbb{Z}_{(p)}$. Formulated in terms of the initial R -valued sequence $\{b_n\}$ this functional equation means that for every $k \geq 0$ and $m \geq 1$, m not divisible by p , we have

$$b_{mp^k-1} - \sum_{s=1}^k p^{s-1} v_s \sigma^s(b_{mp^{k-s}-1}) = mp^k d_{mp^k} \in p^k R \otimes \mathbb{Z}_{(p)}. \quad (13)$$

Let's first prove that $c_{p^k-1} \in p^{k-1} R$ for all $k \geq 1$. We shall first prove that

$$c_{p^k-1} = p^{k-1} v_k + p^k d_{p^k} - \sum_{i=1}^{k-1} \sigma^i(c_{p^{k-i}-1}) p^i d_{p^i}. \quad (14)$$

For $k = 1$ this formula follows from $b_{p-1} = c_{p-1} = v_1 + p d_p$. We will now do induction in k . Subtracting the two expressions

$$b_{p^k-1} = c_{p-1} \sigma(b_{p^{k-1}-1}) + c_{p^2-1} \sigma^2(b_{p^{k-2}-1}) + \dots + c_{p^k-1}$$

and

$$b_{p^k-1} = v_1 \sigma(b_{p^{k-1}-1}) + p v_2 \sigma^2(b_{p^{k-2}-1}) + \dots + p^{k-1} v_k + p^k d_k$$

(coming from (10) and (13) respectively) and using (14) for all indices smaller than k we obtain that

$$\begin{aligned} c_{p^k-1} - p^{k-1} v_k - p^k d_p &= \sum_{i=1}^{k-1} (p^{i-1} v_i - c_{p^i-1}) \sigma^i(b_{p^{k-i}-1}) \\ &= \sum_{i=1}^{k-1} \left(-p^i d_{p^i} + \sum_{j=1}^{i-1} \sigma^j(c_{p^{i-j}-1}) p^j d_{p^j} \right) \sigma^i(b_{p^{k-i}-1}) \\ &= - \sum_{i=1}^{k-1} p^i d_{p^i} \left(\sigma^i(b_{p^{k-i}-1}) - \sum_{j=1}^{k-i} \sigma^i(c_{p^j-1}) \sigma^{i+j}(b_{p^{k-i-j}-1}) \right) \\ &= - \sum_{i=1}^{k-1} p^i d_{p^i} \sigma^i(c_{p^{k-i}-1}), \end{aligned}$$

which proves (14) for this k . The fact that $c_{p^k-1} \in p^{k-1} R \otimes \mathbb{Z}_{(p)}$ follows from (14) by induction on k . It remains to observe that $R \cap (p^k R \otimes \mathbb{Z}_{(p)}) = p^k R$ for every k .

So far we proved (11) with $m = p$ for all k . Now consider the case of $m > 1$ not divisible by p . Suppose that for some $k > 0$ and for all such m we knew that

$$\begin{aligned} b_{mp^k-1} - c_{p-1} \cdot \sigma(b_{mp^{k-1}-1}) - c_{p^2-1} \cdot \sigma^2(b_{mp^{k-2}-1}) - \dots - c_{p^k-1} \cdot \sigma^k(b_{m-1}) \\ = \sum_{\substack{m = m' * m'' \\ m' > 1, m'' \geq 0}} c_{m' p^k-1} \cdot \sigma^{k+\ell(m')}(b_{m''}) \end{aligned} \quad (15)$$

belongs to $p^k R$. Then (11) for this k would follow by induction on the length $\ell(m)$.

It remains to prove that the left-hand side in (15) belongs to $p^k R$. Since it obviously belongs to R and $R \cap (p^k R \otimes \mathbb{Z}_{(p)}) = p^k R$, it is enough to show that the left-hand side in (15) belongs to $p^k R \otimes \mathbb{Z}_{(p)}$. Consider $\tilde{f}(x) = \sum_{k=0}^{\infty} \frac{b_{p^k-1}}{p^k} x^{p^k}$ and the p -typical formal group law $\tilde{F}(x, y) = \tilde{f}^{-1}(\tilde{f}(x) + \tilde{f}(y))$. Observe that \tilde{F} has coefficients in $R \otimes \mathbb{Z}_{(p)}$ because we have the functional equation

$$\tilde{f}(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s \cdot (\sigma^s \tilde{f})(x) = \sum_{k=0}^{\infty} d_{p^k} x^{p^k}.$$

By [1, Theorem 16.4.14 and Remark 16.4.15] \tilde{F} is isomorphic to F over $R \otimes \mathbb{Z}_{(p)}$. Observe that we have another functional equation for \tilde{f} : with $v'_s = \frac{c_{p^s-1}}{p^{s-1}} \in R$ one has

$$\tilde{f}(x) - \frac{1}{p} \sum_{s=1}^{\infty} v'_s \cdot (\sigma^s \tilde{f})(x) = x.$$

Since F and \tilde{F} are isomorphic, by part (iii) of Hazewinkel's functional equation lemma we must have that the coefficients of the power series $f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v'_s \cdot (\sigma^s f)(x)$ also lie in $R \otimes \mathbb{Z}_{(p)}$, which is precisely what we wanted to prove. \square

3 Computing local invariants

In this section R is the ring of integers of a complete absolutely unramified discrete valuation field K of characteristic zero and residue characteristic $p > 0$, equipped with a Frobenius endomorphism $\sigma : K \rightarrow K$ which is the lift of the p th power endomorphism on the residue field R/pR . The valuation is denoted by $\text{ord}_p : K \rightarrow \mathbb{Z} \cup +\infty$.

Let $\{v_s; s \geq 1\}$ be a sequence of elements of R and $g \in x + x^2R[[x]]$ be a power series. The functional equation

$$g(x) = f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s (\sigma^s f)(x)$$

allows one to recover $f(x) \in x + x^2K[[x]]$. Hazewinkel's functional equation lemma tells us that the formal group law $F(x, y) = f^{-1}(f(x) + f(y))$ has coefficients in R ([1, §2.2 (i)]). Moreover, since R is a $\mathbb{Z}_{(p)}$ -algebra, every formal group law over R can be constructed this way ([1, Proposition 20.1.3]). Two formal group laws with the same $\{v_s; s \geq 1\}$ and different $g(x)$ are strictly isomorphic over R ([1, §2.2 (ii)]). Conversely, if a formal group law over R satisfies a functional equation with some $\{v_s; s \geq 1\}$ then every formal group law strictly isomorphic to it over R satisfies a functional equation with the same $\{v_s; s \geq 1\}$ but different $g(x)$ ([1, §2.2 (ii) and (iii)]).

Honda ([2], [1, §20.3]) gave the following method to describe all sequences $\{v_s; s \geq 1\}$ with which a given formal group law $F(x, y) = f^{-1}(f(x) + f(y)) \in R[[x, y]]$ satisfies

$$f(x) - \frac{1}{p} \sum_{s=1}^{\infty} v_s (\sigma^s f)(x) \in R[[x]]. \quad (16)$$

(As we just explained, the set of such sequences corresponds to the strict isomorphism class of F .) Denote by $K_\sigma[[T]]$ the ring of 'non-commutative' power series with coefficients in K , where the multiplication satisfies $Ta = \sigma(a)T$ for $a \in K$. We put the word *non-commutative* in commas because this ring is commutative whenever σ is the identity endomorphism, e.g. when $K = \mathbb{Q}_p$. We denote by $R_\sigma[[T]] \subset K_\sigma[[T]]$ the subring of power series with coefficients in R . With (16) one associates an element $\eta_v = p - \sum_{s=1}^{\infty} v_s T^s \in R_\sigma[[T]]$. Then every other sequence $v' = \{v'_s; s \geq 1\}$ with which (16) also holds comes as $\eta_{v'} = \theta \eta_v$ where $\theta \in 1 + R_\sigma[[T]]T$.

The height of $F(x, y)$ can be computed as

$$h = \inf\{s \geq 1 : v_s \in R^\times\} \quad (17)$$

and is invariant under strict isomorphisms. If $h < \infty$, then by the formal Weierstrass preparation lemma ([1, Lemma 20.3.13]) there exist a unique power series $\theta \in 1 + R_\sigma[[T]]T$ and elements $\alpha_1, \dots, \alpha_{h-1} \in pR$, $\alpha_h \in R^\times$ such that $\theta \eta_v = p - \sum_{i=1}^h \alpha_i T^i$. The Eisenstein polynomial in the right-hand side of this expression is the characteristic polynomial of $F(x, y)$. It was denoted by $\Psi_F(T)$ in Section 1. The strict isomorphism classes of formal group laws of finite height over R correspond bijectively to such polynomials ([1, Theorem 20.3.12]).

Proof of Theorem 2. Let $\{c_n; n \geq 0\}$ be the p -sequence associated with $\{b_n; n \geq 0\}$. By Theorem 1 we have $c_{p^s-1} \in p^{s-1}R$ for all $s \geq 1$ and (16) is satisfied with the sequence $v_s = \frac{c_{p^s-1}}{p^{s-1}} \in R$. We can now rewrite (17) as

$$h = \inf\{s \geq 1 : \text{ord}_p(c_{p^s-1}) = s - 1\}. \quad (18)$$

(i) Let's denote $\mu_n = b_{p^n-1}/p^n$, $\kappa_n = c_{p^n-1}/p^n$. Dividing the identity

$$b_{p^n-1} = c_{p-1} \sigma(b_{p^{n-1}}) + c_{p^2-1} \sigma^2(b_{p^{n-1}-1}) + \dots + c_{p^n-1} \quad (19)$$

by p^n we obtain

$$\mu_n = \kappa_1 \sigma(\mu_{n-1}) + \kappa_2 \sigma(\mu_{n-2}) + \dots + \kappa_{n-1} \sigma^{n-1}(\mu_1) + \kappa_n. \quad (20)$$

When $h = \infty$ then $\kappa_n \in R$ for all n due to (18), and therefore $\mu_n \in R$ for all n by induction. From now on we assume that $h < \infty$. We then have $\text{ord}_p(\kappa_i) \geq 0$ for $i < h$, $\text{ord}_p(\kappa_h) = -1$ and $\text{ord}_p(\kappa_i) \geq -1$ for $i > h$. It follows that $\text{ord}_p(\mu_i) \geq 0$ when $i < h$ and $\text{ord}_p(\mu_h) = -1$. We will prove by induction that $\text{ord}_p(\mu_n) \geq -\lfloor \frac{n}{h} \rfloor$ with equality when $h|n$. Suppose this inequality holds for all indices less than n . Then for $1 \leq i < h$ we have $\text{ord}_p(\kappa_i \sigma^i(\mu_{n-i})) = \text{ord}_p(\kappa_i) + \text{ord}_p(\mu_{n-i}) \geq 0 - \lfloor \frac{n-i}{h} \rfloor \geq -\lfloor \frac{n}{h} \rfloor$ with strict inequality when $h|n$. For $i > h$ we have $\text{ord}_p(\kappa_i \sigma^i(\mu_{n-i})) = \text{ord}_p(\kappa_i) + \text{ord}_p(\mu_{n-i}) \geq -1 - \lfloor \frac{n-i}{h} \rfloor = -\lfloor \frac{n-(i-h)}{h} \rfloor \geq -\lfloor \frac{n}{h} \rfloor$, where the last inequality is again strict when $h|n$. When $i = h$ we have

$$\text{ord}_p(\kappa_h \sigma^h(\mu_{n-h})) = \text{ord}_p(\kappa_h) + \text{ord}_p(\mu_{n-h}) \begin{cases} = -1 - \lfloor \frac{n-h}{h} \rfloor = -\lfloor \frac{n}{h} \rfloor & \text{when } h|n, \\ \geq -1 - \lfloor \frac{n-h}{h} \rfloor = -\lfloor \frac{n}{h} \rfloor & \text{when } h \nmid n. \end{cases}$$

Summarizing the above we get that $\text{ord}_p(\mu_n) \geq -\lfloor \frac{n}{h} \rfloor$ with equality when $h|n$, which proves the first part of the theorem.

(ii) We have $\beta_{kh} = p^k \mu_{kh}$. From (20) with $n = h$ we find that $p\mu_h \equiv p\kappa_h \pmod{p}$. Computation in part (i) shows that modulo p

$$p^k \mu_{kh} \equiv p^k \kappa_h \sigma^h(\mu_{(k-1)h}) = (p\kappa_h)(p^{k-1} \sigma^h(\mu_{(k-1)h})) \equiv \dots \equiv \prod_{i=0}^{k-1} (p \sigma^{ih}(\kappa_h)) \equiv \prod_{i=0}^{k-1} \sigma^{ih}(\beta_h).$$

(iii) The characteristic polynomial provides us with the shortest possible functional equation (16) where $v_s = \alpha_s$ for $s \leq h$ and $v_s = 0$ for $s > h$. Therefore for every $n \geq 0$

$$p^n \mid b_{p^n-1} - \sum_{s=1}^h p^{s-1} \alpha_s \sigma^s(b_{p^n-s-1}).$$

Let's consider the last congruence for $n = kh + i$ where $0 \leq i < h$ and divide it by $p^{k(h-1)+i}$:

$$p^k \mid \frac{b_{p^{kh+i}-1}}{p^{k(h-1)+i}} - \sum_{s=1}^h \frac{\alpha_s}{p} \frac{\sigma^s(b_{p^{kh+i-s}-1})}{p^{k(h-1)+i-s}}.$$

With the notation $\beta_n = b_{p^n-1}/p^{n-\lfloor \frac{n}{h} \rfloor}$ we rewrite the last congruence as

$$p^k \mid \beta_{kh+i} - \sum_{s=1}^h \frac{\alpha_s}{p} p^{\tilde{\varepsilon}_{is}} \sigma^s(\beta_{kh+i-s}) \quad \text{with} \quad \tilde{\varepsilon}_{is} = \begin{cases} 0, & s \leq i, \\ 1, & s > i. \end{cases}$$

Substituting $s = j + 1$ and combining all congruences with $i = 0, \dots, h-1$ we obtain

$$p^k \mid \begin{pmatrix} \beta_{kh} \\ \beta_{kh+1} \\ \vdots \\ \beta_{kh+h-2} \\ \beta_{kh+h-1} \end{pmatrix} - D_k \begin{pmatrix} \alpha_1/p \\ \alpha_2/p \\ \vdots \\ \alpha_{h-1}/p \\ \alpha_h \end{pmatrix},$$

where D_k is the matrix defined in the statement of part (iii). By (i) all $\beta_n \in R$, hence all entries of D_k belong to R . Therefore it only remains to check that $p \nmid \det(D_k)$. The entries of D_k are 0 modulo p when $\varepsilon_{ij} = 1$, that is when $i \leq j < h-1$. It means that modulo p the determinant

is congruent (up to sign) to the product of the entries under the main diagonal, which are all equal to $\sigma^i(\beta_{kh})$ for $i = 1, \dots, h-1$, times the upper-right entry, which is equal to $\sigma^h(\beta_{(k-1)h})$. Using (ii) we obtain

$$\begin{aligned} \det D_k &\equiv (-1)^{h-1} \prod_{i=1}^{h-1} \sigma^i(\beta_{kh}) \cdot \sigma^h(\beta_{(k-1)h}) \\ &\equiv (-1)^{h-1} \prod_{i=1}^{h-1} \prod_{j=0}^{k-1} \sigma^{i+jh}(\beta_h) \cdot \prod_{j=0}^{k-2} \sigma^{h(1+j)}(\beta_h) = (-1)^{h-1} \prod_{s=1}^{kh-1} \sigma^s(\beta_h) \pmod{p}. \end{aligned}$$

□

4 Applications and examples

4.1 Formal group laws attached to L-functions

For the purposes of this paper, an *L-function* is a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

with integral coefficients $a_n \in \mathbb{Z}$, which has an Euler product

$$L(s) = \prod_{p \text{ prime}} \mathcal{P}_p(p^{-s})^{-1},$$

where $\mathcal{P}_p(T) \in 1 + T\mathbb{Z}[T]$ is a polynomial for every prime number p . The Euler product is understood formally, that is we don't care about convergence and the sequence $\{a_n; n \geq 1\}$ is determined by the rules:

$$\begin{aligned} a_{mn} &= a_m a_n \quad \text{when} \quad (m, n) = 1, \\ a_{p^s} + \gamma_1(p) a_{p^{s-1}} + \dots + \gamma_{d(p)}(p) a_{p^{s-d}} &= 0 \quad \text{where} \quad \mathcal{P}_p(T) = 1 + \sum_{i=1}^{d(p)} \gamma_i(p) T^i. \end{aligned} \quad (21)$$

(By convention, we assume $a_k = 0$ when $k \notin \mathbb{Z}_{\geq 1}$.)

To an L-function one associates an one-dimensional formal group law over \mathbb{Q} by the formula

$$F_L(x, y) = f^{-1}(f(x) + f(y)), \quad f(x) = \sum_{n=1}^{\infty} \frac{a_n}{n} x^n. \quad (22)$$

We shall now prove

Proposition 3. *For a fixed prime p , we have $F \in \mathbb{Z}_{(p)}[[x, y]]$ if and only if*

$$Q(T) := p \mathcal{P}_p\left(\frac{T}{p}\right) \in p + T\mathbb{Z}[T]. \quad (23)$$

Assume that (23) holds. If $Q \equiv 0 \pmod{p}$ then F is strictly isomorphic to \mathbb{G}_a over $\mathbb{Z}_{(p)}$, and otherwise the local characteristic polynomial $\Psi_F(T)$ at p is equal to the unique monic Eisenstein factor of $Q(T)$ in the ring $\mathbb{Z}_p[T]$ of polynomials with p -adic integral coefficients and the height $h = \deg \Psi_F$ is equal to the highest power of T that divides $\overline{Q}(T) = Q(T) \pmod{p}$.

The following lemma enables us to describe the p -sequence associated to the (shifted) sequence of coefficients of an L-function.

Lemma. *Let $\{a_n; n \geq 1\}$ be a sequence of integers with $a_1 = 1$. Fix a prime number p . Let $\{c_n; n \geq 0\}$ be the p -sequence associated to the shifted sequence $\{b_n = a_{n+1}; n \geq 0\}$.*

(i) *We have*

$$a_{mp^k} = a_m a_{p^k} \quad \text{for all } m \text{ not divisible by } p \text{ and } k \geq 0 \quad (24)$$

if and only if

$$c_{mp^{k-1}} = 0 \quad \text{for all } m > 1 \text{ not divisible by } p \text{ and } k > 0. \quad (25)$$

(ii) *There is a recurrence relation of the form*

$$a_{p^k} + \gamma_1 a_{p^{k-1}} + \dots + \gamma_d a_{p^{k-d}} = 0 \quad \text{for all } k \geq 0 \quad (26)$$

with some $d \geq 1$ and integers $\gamma_1, \dots, \gamma_d$ (where, by convention, $a_n = 0$ when $n \notin \mathbb{Z}$) if and only if

$$c_{p^i-1} = \begin{cases} -\gamma_i, & 1 \leq i \leq d, \\ 0, & i > d. \end{cases}$$

Proof. (i) \Rightarrow First we prove that (25) follows from (24). Take any $m > 1$ not divisible by p and $k > 0$. We have

$$b_{mp^k-1} = c_{p-1} b_{mp^{k-1}-1} + \dots + c_{p^{k-1}} b_{m-1} + \sum_{\substack{m = m' * m'' \\ m' > 1, m'' \geq 0}} c_{m'p^{k-1}} b_{m''}, \quad (27)$$

where the sum runs over all decompositions $m = m' + p^{\ell(m')} m''$ of the p -adic expansion of m into a concatenation of p -adic expansions of two non-negative integers, of which m' is actually positive because $k > 0$. The condition $m' > 1$ is then satisfied automatically due to the fact that $m > 1$ is not divisible by p . Since $b_{mp^i-1} = b_{p^i-1} b_{m-1}$ for $i \geq 0$ due to (24), subtracting from (27) the equality $b_{p^k-1} = c_{p-1} b_{p^{k-1}-1} + \dots + c_{p^{k-1}}$ multiplied by b_{m-1} yields

$$\sum_{\substack{m = m' * m'' \\ m' > 1, m'' \geq 0}} c_{m'p^{k-1}} b_{m''} = 0.$$

If m had one p -adic digit the sum here would have just one term $c_{mp^{k-1}} b_0 = c_{mp^{k-1}}$, so we get $c_{mp^{k-1}} = 0$. Now (25) follows by induction on the length $\ell(m)$ of the p -adic expansion of m .

\Leftarrow Suppose now that (25) holds. When $m = 1$ or $k = 0$ (24) holds automatically. Take any $m > 1$ not divisible by p and $k > 0$ and consider (27) once again. The rightmost sum then vanishes due to (25) since $m' \equiv m \not\equiv 0 \pmod{p}$ for each term. Therefore we get

$$b_{mp^k-1} = c_{p-1} b_{mp^{k-1}-1} + \dots + c_{p^{k-1}} b_{m-1}.$$

If $k = 1$ we have $b_{mp-1} = c_{p-1} b_{m-1} = b_{p-1} b_{m-1}$. For $k > 1$ we proceed by induction:

$$b_{mp^k-1} = (c_{p-1} b_{p^{k-1}-1} + \dots + c_{p^{k-1}}) b_{m-1} = b_{p^k-1} b_{m-1},$$

which proves (24).

(ii) follows immediately from the equalities $a_{p^k} = c_{p-1} a_{p^{k-1}} + c_{p^{k-1}} a_{p^{k-2}} + \dots + c_{p^{k-1}}$ for every $k \geq 1$ and $a_1 = 1$. \square

Proof of Proposition 3. Let $\{c_n; n \geq 0\}$ be the p -sequence associated with $\{b_n = a_{n+1}; n \geq 0\}$. By (21) and part (i) in the preceding lemma we have $c_{mp^k-1} = 0$ for every $m > 1$ not divisible by p and any $k > 0$. By (21) and part (ii) in the preceding lemma we have $c_{p^k-1} = -\gamma_k(p)$ for $k \geq 1$. Hence condition (3) in Theorem 1 is equivalent to $p^{k-1}|\gamma_k(p)$ for $k \geq 1$, which is in turn equivalent to (23) because $Q(T) = p + \sum_{i=1}^{d(p)} \frac{\gamma_i(p)}{p^{i-1}} T^i$. The characteristic polynomial is the unique Eisenstein factor of $Q(T)$ by the construction reminded at the beginning of Section 3: we have $Q = \eta_v$ for the sequence $v = \{v_i = \frac{c_{p^i-1}}{p^{i-1}}; i \geq 1\}$. \square

4.2 Artin–Mazur formal groups

In [6] Artin and Mazur associated formal groups to cohomology groups of algebraic schemes. In [7] Stienstra computed explicit coordinatizations of Artin–Mazur functors related to the middle cohomology of complete intersections and double coverings of projective spaces. Stienstra’s formal group laws are integral over the base ring and coefficients of their logarithms are always given as coefficients of powers of a polynomial (see Theorems 1 and 2 in *loc. cit.*).

Proposition 4. *Let R be a characteristic 0 ring and $V(x) \in R[x_1^\pm, \dots, x_m^\pm]$ be a Laurent polynomial. Assume that Newton polytope $\Delta(V) \subset \mathbb{R}^m$ contains a unique internal integral point $\{w\} = \Delta(F)^\circ \cap \mathbb{Z}^m$. Consider the R -valued sequence*

$$b_n = \text{the coefficient of } x^{nw} \text{ in } V(x)^n.$$

Assume that R equipped with a p th power Frobenius endomorphism and let $\{c_n; n \geq 0\}$ be the p -sequence attached to $\{b_n; n \geq 0\}$. Then one has

$$c_n \in p^{\ell(n)-1} R \quad (28)$$

for every $n \geq 0$.

The proof was essentially given in [5, Lemma 1] and the generalization to rings with Frobenius endomorphism stated here is straightforward. Notice that congruences (28) are stronger than (3). Therefore it follows from Theorem 1 that

Corollary. *The formal group law*

$$F_V(x, y) = f^{-1}(f(x) + f(y)), \quad f(x) = \sum_{n=1}^{\infty} \frac{b_{n-1}}{n} x^n$$

has coefficients in $R \otimes \mathbb{Z}_{(p)}$ whenever we can equip R with a p th power Frobenius endomorphism.

According to Stienstra, in case $V(x)$ is a homogeneous polynomial this formal group law is a coordinatization of the Artin–Mazur formal group attached to the middle cohomology of the hypersurface of zeroes of $V(x)$. Integrality of such formal group laws was established in [7], but our case is more general and methods are elementary.

In [8] Stienstra proved a generalization of the Atkin and Swinnerton-Dyer congruences when R is of finite type over \mathbb{Z} . Such congruences allow one to establish isomorphism of Artin–Mazur formal groups and formal groups attached to respective L-functions. Let us demonstrate how Theorem 2 works in an example with a double covering. Consider a K3 surface \mathfrak{X} (called \mathcal{A}' in [9]) given by

$$Y^2 = T_0 T_1 T_2 (T_1 - T_2)(T_1 T_2 - T_0^2).$$

According to a computation in *loc. cit.*, for every $p \neq 2$ the respective Euler factor of the L-function associated to $H^2(\mathfrak{X})$ has the shape

$$\mathcal{P}_p(T) = (1 - pT)^{20} (1 + A_p T + (-1)^{\frac{p-1}{2}} p^2 T^2)$$

where

$$A_p = \begin{cases} 0, & \text{if } p \equiv 3 \pmod{4}, \\ 2p - 4a^2, & \text{if } p \equiv 1 \pmod{4} \text{ } (p = a^2 + 4b^2, a, b \in \mathbb{Z}). \end{cases}$$

The conditions of Proposition 3 are satisfied since

$$Q(T) = p\mathcal{P}_p(T/p) = (1-T)^{20}(p + A_p T + (-1)^{\frac{p-1}{2}} p T^2) \in \mathbb{Z}[T].$$

By Proposition 3 the local characteristic polynomial of this formal group law at p is given by

$$\Psi(T) = \begin{cases} p, & \text{if } p \equiv 3 \pmod{4}, \\ p - \alpha T, & \text{if } p \equiv 1 \pmod{4} \text{ } (\alpha^2 + A_p \alpha + p^2 = 0, \alpha \in \mathbb{Z}_p^\times). \end{cases} \quad (29)$$

On the other hand, by [7, Theorem 2] the coefficients of the logarithm of a coordinatization of the Artin–Mazur formal group associated to $H^2(\mathfrak{X})$ are given by

$$\begin{aligned} b_n &= \begin{cases} 0, & n \text{ odd}, \\ \text{the coefficients of } T_0^n T_1^n T_2^n \text{ in } (T_0 T_1 T_2)^{n/2} (T_1 - T_2)^{n/2} (T_1 T_2 - T_0^2)^{n/2}, & n \text{ even}, \end{cases} \\ &= \begin{cases} 0, & 4 \nmid n, \\ \binom{n/2}{n/4}^2, & 4 \mid n. \end{cases} \end{aligned}$$

We apply formula (7) to obtain a p -adic analytic formula for the coefficient $\alpha \in \mathbb{Z}_p^\times$ in (29) when $p \equiv 1 \pmod{4}$:

$$\alpha = \lim_{k \rightarrow \infty} \frac{b_{p^k-1}}{b_{p^{k-1}-1}} = \lim_{k \rightarrow \infty} \frac{\Gamma_p(\frac{p^k-1}{2} + 1)^2}{\Gamma_p(\frac{p^k-1}{4} + 1)^4} = \frac{\Gamma_p(\frac{1}{2})^2}{\Gamma_p(\frac{3}{4})^4} = \frac{(-1)^{\frac{p+1}{2}}}{\Gamma_p(\frac{3}{4})^4} = -\Gamma_p(\frac{1}{4})^4,$$

where $\Gamma_p(\cdot)$ is the p -adic gamma function (see [10, §IV.2]). It follows that

$$A_p = -\alpha - p\alpha^{-1} = \Gamma_p(\frac{1}{4})^4 + p\Gamma_p(\frac{3}{4})^4.$$

4.3 Hypergeometric formal group laws

Consider a finite system of integral weights on positive integers $\gamma = \{\gamma_\nu; \nu \geq 1\}$. By this we mean that each $\gamma_\nu \in \mathbb{Z}$ and $\gamma_\nu = 0$ for all but finitely many ν . We assume that γ satisfies the condition

$$\sum_{\nu \geq 1} \nu \gamma_\nu = 0. \quad (30)$$

Following [11], we associate to γ the sequence of rational numbers $u_n = \prod_{\nu \geq 1} (\nu n)^{\gamma_\nu}$, $n \geq 0$. One has $\text{ord}_p(u_n) = \sum_{i=1}^{\infty} \mathcal{L}(\frac{n}{p^i})$ where

$$\mathcal{L}(t) = \sum_{\nu} \gamma_\nu \lfloor \nu t \rfloor$$

is the associated *Landau function*. This function is right-continuous and locally constant. Condition (30) implies that $\mathcal{L}(t)$ is periodic with period 1. It is named after Emil Landau who observed that the sequence $\{u_n; n \geq 0\}$ is integral if and only if

$$\mathcal{L}(t) \geq 0 \quad \text{for all } t. \quad (31)$$

Let $N = \text{l.c.m.}\{\nu \mid \gamma_\nu \neq 0\}$. Assuming the integrality of $\{u_n; n \geq 0\}$, we will give a criterion of integrality of the rational formal group law given by

$$F_\gamma(x, y) = f^{-1}(f(x) + f(y)), \quad f(x) = \sum_{n=0}^{\infty} u_n \frac{x^{Nn+1}}{Nn+1} = \int \sum u_n x^{Nn} dx.$$

Proposition 5. Suppose the system of weights $\gamma = \{\gamma_\nu; \nu \geq 1\}$ satisfies conditions (30) and (31).

(i) For a prime $p > N$ let $d = \min\{m > 0 \mid p^m \equiv 1 \pmod{N}\}$ be the order of p in the multiplicative group of invertible residues modulo N . For each $1 \leq a < d$ let $1 \leq m_a < N$ be the unique number such that $m_a p^a \equiv 1 \pmod{N}$. The coefficients of F_γ are p -integral if and only if

$$\lambda_a := \text{ord}_p(u_{\frac{m_a p^a - 1}{N}}) \geq a \quad \text{for each } 1 \leq a < d. \quad (32)$$

(ii) Assume (32) is satisfied. If $\lambda_{d-1} = d - 1$, the height of F_γ at p equals d and the local characteristic polynomial is given by

$$\Psi_{F_\gamma}(T) = p - \xi T^d \quad \text{with} \quad \xi = (-1)^{(\gamma_2+1)d-1} \prod_{\nu} \prod_{a=0}^{d-1} \Gamma_p \left(1 - \frac{[m_a]_{(N/\nu)}}{N/\nu} \right)^{\gamma_\nu}, \quad (33)$$

where $1 \leq [m_a]_{(N/\nu)} < N/\nu$ is the unique number congruent to m_a modulo N/ν . If $\lambda_{d-1} \geq d$ then the height at p is infinite.

(iii) The numbers λ_a for $0 \leq a < d$ and hence the condition of integrality (32) and the height depend only on the residue class $p \pmod{N}$.

Proof. We write $f(x) = \sum_{n=1}^{\infty} b_{n-1} \frac{x^n}{n}$ where $b_n = u_{\frac{n}{N}}$ if $N \mid n$ and $b_n = 0$ otherwise. Let $\{c_n\}$ be the p -sequence associated to $\{b_n\}$. It is easy to see that $c_n = 0$ when $N \nmid n$. We also observe that $c_{m_a p^a - 1} = b_{m_a p^a - 1}$ for each $1 \leq a < d$. Indeed, since m_a is the smallest positive integer with the property $m_a p^a \equiv 1 \pmod{N}$ it is impossible to divide the p -adic expansion of $m_a p^a - 1$ into two parts so that each part represents a number divisible by N . The necessity of condition (32) in (i) now follows from Theorem 1.

We will prove that (32) is sufficient for p -integrality and simultaneously prove part (ii). Assume that (32) holds. Note that jumps of $\mathcal{L}(t)$ happen at rational points whose denominators divide N . Therefore $\mathcal{L}(t) = 0$ for $0 \leq t < \frac{1}{N}$. Using this fact and periodicity of $\mathcal{L}(t)$ we see that

$$\begin{aligned} \text{ord}_p(b_{m_a p^a - 1}) &= \sum_{i=1}^{\infty} \mathcal{L}\left(\frac{m_a p^a - 1}{N p^i}\right) = \sum_{i=1}^a \mathcal{L}\left(\frac{m_a p^a - 1}{N p^i}\right) \\ &\quad (p^i < m_a p^a \Rightarrow i \leq a \text{ since } m_a < N < p) \\ &= \sum_{i=1}^a \mathcal{L}\left(\frac{m_a p^{a-i} - 1}{N}\right) \quad (\text{because } \lfloor \frac{m_a p^a - 1}{p^i} \rfloor = m_a p^{a-i} - 1) \\ &= \sum_{i=1}^a \mathcal{L}\left(\frac{p^{d-i} - 1}{N}\right) \quad (\text{because } m_a \equiv p^{d-a} \pmod{N}). \end{aligned}$$

Due to the periodicity of the Landau function this number depends only on $p \pmod{N}$ as claimed in (iii). Same arguments yield $\text{ord}_p(b_{p^d - 1}) = \sum_{i=1}^{d-1} \mathcal{L}\left(\frac{p^d - 1}{N p^i}\right) = \sum_{i=1}^{d-1} \mathcal{L}\left(\frac{p^{d-i} - 1}{N}\right) = \text{ord}_p(b_{m_{d-1} p^{d-1} - 1})$, which is $\geq d - 1$ by (32).

Let $k = a + sd$ with $0 \leq a < d$, $s \geq 0$ and assume that $m \equiv m_a \pmod{N}$. For the rest of the proof we will need the following two observations:

$$\text{ord}_p(b_{m p^k - 1}) \geq \text{ord}_p(b_{m_a p^k - 1}) \quad (34)$$

and

$$\text{ord}_p(b_{m p^k - 1}) = s \text{ord}_p(b_{p^d - 1}) + \text{ord}_p(b_{m_a p^a - 1}). \quad (35)$$

We prove (34) as follows

$$\begin{aligned} \text{ord}_p(b_{mp^k-1}) &= \sum_{i=1}^{k+\ell(m)-1} \mathcal{L}\left(\frac{mp^k-1}{Np^i}\right) \stackrel{\text{by (31)}}{\geq} \sum_{i=1}^k \mathcal{L}\left(\frac{mp^k-1}{Np^i}\right) = \sum_{i=1}^k \mathcal{L}\left(\frac{mp^{k-i}-1}{N}\right) \\ &\stackrel{m \equiv m_a \pmod{N}}{=} \sum_{i=1}^k \mathcal{L}\left(\frac{m_ap^{k-i}-1}{N}\right) = \sum_{i=1}^k \mathcal{L}\left(\frac{m_ap^k-1}{Np^i}\right) = \text{ord}_p(b_{m_ap^k-1}). \end{aligned}$$

For (35) we observe that

$$\begin{aligned} \text{ord}_p(b_{mp^k-1}) - \text{ord}_p(b_{mp^{k-d}-1}) &= \sum_{i=1}^{k+\ell(m)-1} \mathcal{L}\left(\frac{mp^{k-i}-1}{N}\right) - \sum_{j=1}^{k-d+\ell(m)-1} \mathcal{L}\left(\frac{mp^{k-d-j}-1}{N}\right) \\ &\stackrel{i=j+d}{=} \sum_{i=1}^d \mathcal{L}\left(\frac{mp^{k-i}-1}{N}\right) = \sum_{i=1}^d \mathcal{L}\left(\frac{p^{d-i}-1}{N}\right) = \text{ord}_p(b_{p^d-1}). \end{aligned}$$

When $\text{ord}_p(b_{p^d-1}) \geq d$ then (34), (35) and (32) yield

$$\text{ord}_p(b_{mp^k-1}) \geq \text{ord}_p(b_{m_ap^k-1}) = sd + \text{ord}_p(b_{m_ap^a-1}) \geq sd + a = k,$$

hence $f(x) \in \mathbb{Z}_{(p)}[[x]]$ and F_γ is strictly isomorphic to $x + y$ over $\mathbb{Z}_{(p)}$.

It remains to consider the case $\text{ord}_p(b_{p^d-1}) = d - 1$. Then by (35) we have $\text{ord}_p(b_{p^{sd-1}}) = s \text{ord}_p(b_{p^d-1}) = s(d - 1)$. If F_γ were p -integral then by (i) in Theorem 2 the height would equal $h = d$ and by (iv) in Theorem 2 the characteristic polynomial would equal $\Psi_p(T) = p - \xi T^d$ with $\xi \in \mathbb{Z}_p^\times$ is such that $\xi \equiv \frac{1}{p^{d-1}} \frac{b_{p^{sd-1}}}{b_{p^{(s-1)d-1}}} \pmod{p^s}$ for each $s \geq 1$. We shall show that, more generally, for $k \geq d$ and m such that $mp^k \equiv 1 \pmod{N}$ one has

$$\frac{b_{mp^k-1}}{p^{d-1}b_{mp^{k-d}-1}} \equiv \xi \pmod{p^{k+1-d}} \quad (36)$$

with the p -adic unit ξ given in (33). Notice that (36) implies that $\text{ord}_p(b_{mp^k-1} - \xi p^{d-1} b_{mp^{k-d}-1}) \geq (k + 1 - d) + (d - 1) + \text{ord}_p(b_{mp^{k-d}-1}) \geq k$ for all $k \geq d$. Since for $0 \leq k < d$ we also have $\text{ord}_p(b_{mp^k-1}) \geq \text{ord}_p(b_{m_k p^k-1}) \geq k$ by (34) and (32), we obtain that

$$f(x) - \frac{1}{p} \xi f(x^{p^d}) \in \mathbb{Z}_p[[x]]$$

and p -integrality of F_γ then follows from Hazewinkel's functional equation lemma.

The proof of (36) is a routine calculation in p -adic analysis. The p -adic gamma function is defined so that $\frac{n!}{p^{\lfloor n/p \rfloor} \lfloor n/p \rfloor!} = (-1)^{n+1} \Gamma_p(n+1)$ for any $n \geq 1$. Observe that one has $\lfloor \frac{1}{p^i} \lfloor \frac{n}{p} \rfloor \rfloor = \lfloor \frac{n}{p^{i+1}} \rfloor$ for each $i \geq 1$. With $n = \frac{mp^k-1}{N}$ one has $\lfloor \frac{\nu n}{p^i} \rfloor = \frac{mp^{k-i} - [m_i]_{(N/\nu)}}{N/\nu}$ whenever $i < d$. We apply the above formula for the ratio of factorials d times with $0 \leq i < d$ and get

$$\frac{(\nu n)!}{p^* \lfloor \nu n / p^d \rfloor!} = (-1)^{\varepsilon_\nu} \prod_{i=0}^{d-1} \Gamma_p\left(1 + \frac{mp^{k-i} - [m_i]_{(N/\nu)}}{N/\nu}\right) \equiv (-1)^{\varepsilon_\nu} \prod_{i=0}^{d-1} \Gamma_p\left(1 - \frac{[m_i]_{(N/\nu)}}{N/\nu}\right) \pmod{p^{k+1-d}},$$

where

$$\varepsilon_\nu = \sum_{i=0}^{d-1} \left(1 + \frac{mp^{k-i} - [m_i]_{(N/\nu)}}{N/\nu}\right) = d + \frac{\nu}{N} \sum_{i=0}^{d-1} (mp^{k-i} - [m_i]_{(N/\nu)})$$

and we don't need to care about the power of p on the left in this formula since we already know they will sum up to $d - 1$ in (36). Condition (30) implies that $\sum_{\nu} \gamma_{\nu} \varepsilon_{\nu}$ is independent of the pair (m, k) , so we can take it to be $(1, d)$ and get

$$\begin{aligned} \sum_{\nu} \gamma_{\nu} \varepsilon_{\nu} &= \left(\sum_{\nu} \gamma_{\nu} \right) d + \sum_{\nu} \gamma_{\nu} \sum_{i=0}^{d-1} \left\lfloor \frac{\nu(p^d - 1)}{N p^i} \right\rfloor = \left(\sum_{\nu} \gamma_{\nu} \right) d + \sum_{i=0}^{d-1} \mathcal{L}\left(\frac{p^d - 1}{N}\right) \\ &= \left(\sum_{\nu} \gamma_{\nu} \right) d + \text{ord}_p(b_{p^d-1}) = \left(\sum_{\nu} \gamma_{\nu} \right) d + d - 1 \equiv (\gamma_2 + 1)d - 1 \pmod{2}, \end{aligned}$$

which proves our claim. \square

Using the above proposition we can construct formal group laws which are integral at infinitely many primes and non-integral at infinitely many primes. For example, consider the sequence of integers

$$u_n = \frac{(15n)!n!}{(3n)!^2(5n!)^2}.$$

One can easily check that conditions (30) and (31) are satisfied. Here $N = 15$ and the respective formal group law is non-integral at primes p congruent to 7, 11 and 13 modulo 15:

$p \pmod{15}$	1	2	4	7	8	11	13	14
height of F_{γ} at p	1	4	2	-	4	-	-	2

References

- [1] M. Hazewinkel, *Formal groups and applications*, Academic Press, 1978
- [2] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, vol. 22, no. 2 (1970), pp. 213–246
- [3] T. Honda, *Formal groups and zeta-functions*, Osaka J. Math., 5 (1968), pp. 199–213
- [4] T. Honda, *Formal groups obtained from hypergeometric functions*, Osaka J. Math., 9 (1972), pp. 447–462
- [5] A. Mellit, M. Vlasenko, *Dwork's congruences for the coefficients of powers of a Laurent polynomial*, International Journal of Number Theory, 12, no. 2 (2016), pp. 313–321
- [6] M. Artin, B. Mazur, *Formal groups arising from algebraic varieties*, Annales scientifiques de l'É.N.S., 4te série, tome 10, no. 1 (1977), pp. 87–131
- [7] J. Stienstra, *Formal group laws arising from algebraic varieties*, American Journal of Mathematics, 109, no. 5 (1987), pp. 907–925
- [8] J. Stienstra, *Formal groups and congruences for L -functions*, American Journal of Mathematics, 109, no. 6 (1987), pp. 1111–1127
- [9] J. Stienstra, F. Beukers, *On the Picard–Fuchs equation and the formal Brauer group of certain elliptic K3 surfaces*, Math. Ann., 271 (1985), pp. 269–304
- [10] N. Koblitz, *p -adic Numbers, p -adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, 58 (1984)
- [11] F. Rodriguez-Villegas, *Hypergeometric families of Calabi–Yau manifolds*, Calabi–Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun. 38 (2003), pp. 223–231